SCADA:
THREAT LANDSCAPE

Garett Montgomery
DVLabs, TippingPoint
18May2010

GARETT MONTGOMERY

- US Navy: Electronics Technician (Communications)
- Network Security at Naval Postgraduate School
- Masters Degree in Information Assurance
  - CISSP, CWSP, GSNA, SnortCP, C|EH, etc.
- Security Researcher at TippingPoint DVLabs
  - Focusing on SCADA

- *TippingPoint is a leading provider of Intrusion Prevention Systems (IPS).*
  - *www.tippingpoint.com*
- *HP purchased TippingPoint as part of 3com acquisition, April 2010.*
  - *http://www.hp.com/hpinfo/newsroom/press/2009/091111xa.html*

SCADA SYSTEMS – CRITICAL INFRASTRUCTURE

- **S.C.A.D.A.**
  - **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition
  - Computer systems used to monitor and control critical infrastructure .
- **Used around the world by plants and utilities**
  - Power
  - Water
  - Oil & Gas
  - Chemical
- **Critical Infrastructure**
  - Assets essential for functioning of society and economy

THE PROBLEM

– Aging infrastructure in US

- First systems began appearing in the 1960’s – some still in operation
- Typical IT lifespan: 3-5 years. SCADA lifespan: 20-30 years

– Un-patched systems

- Systems cannot go down for patching
- No backup/duplicate systems for testing
- Some systems do not even have the ability to be patched

– Connected to the internet

- SCADA systems were never designed to be connected to the internet
- Symantec report: 100 computers attacked globally per second
- AV-Test.org: 1 million new malware samples appear every month

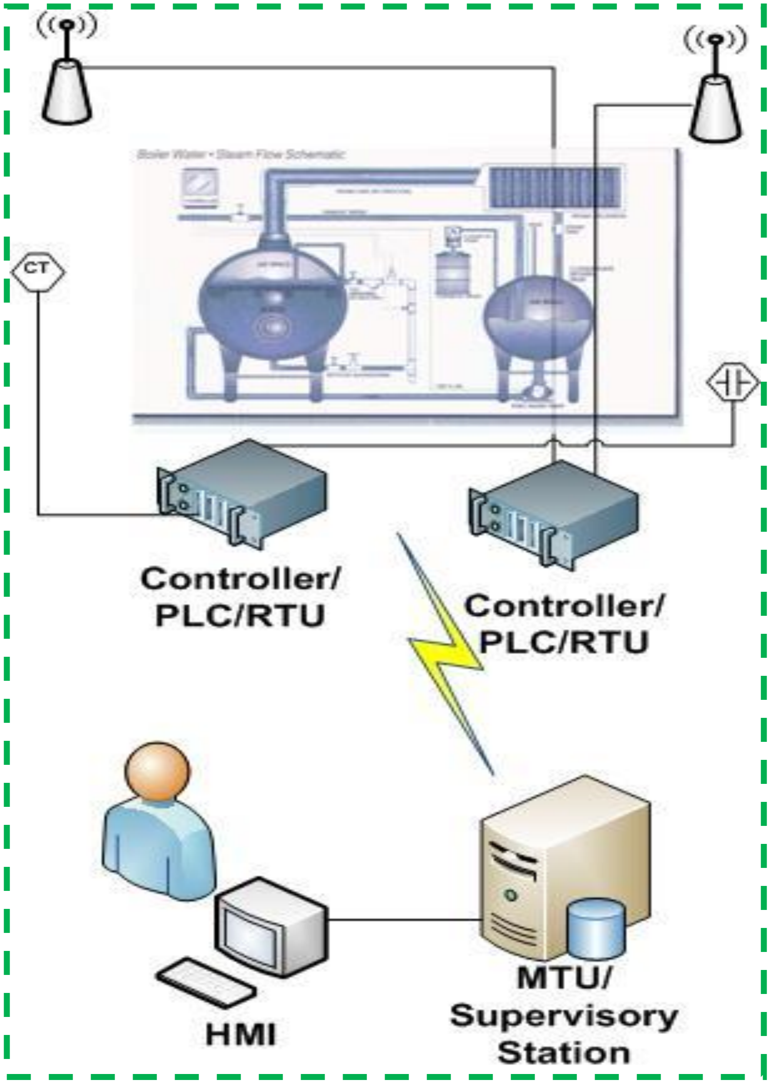
– Security is not a priority

- Terrorists, struggling economy, organized crime/hackers…Risk is increasing
- Security, when considered, is still being added after-the-fact

SCADA SYSTEM COMPONENTS

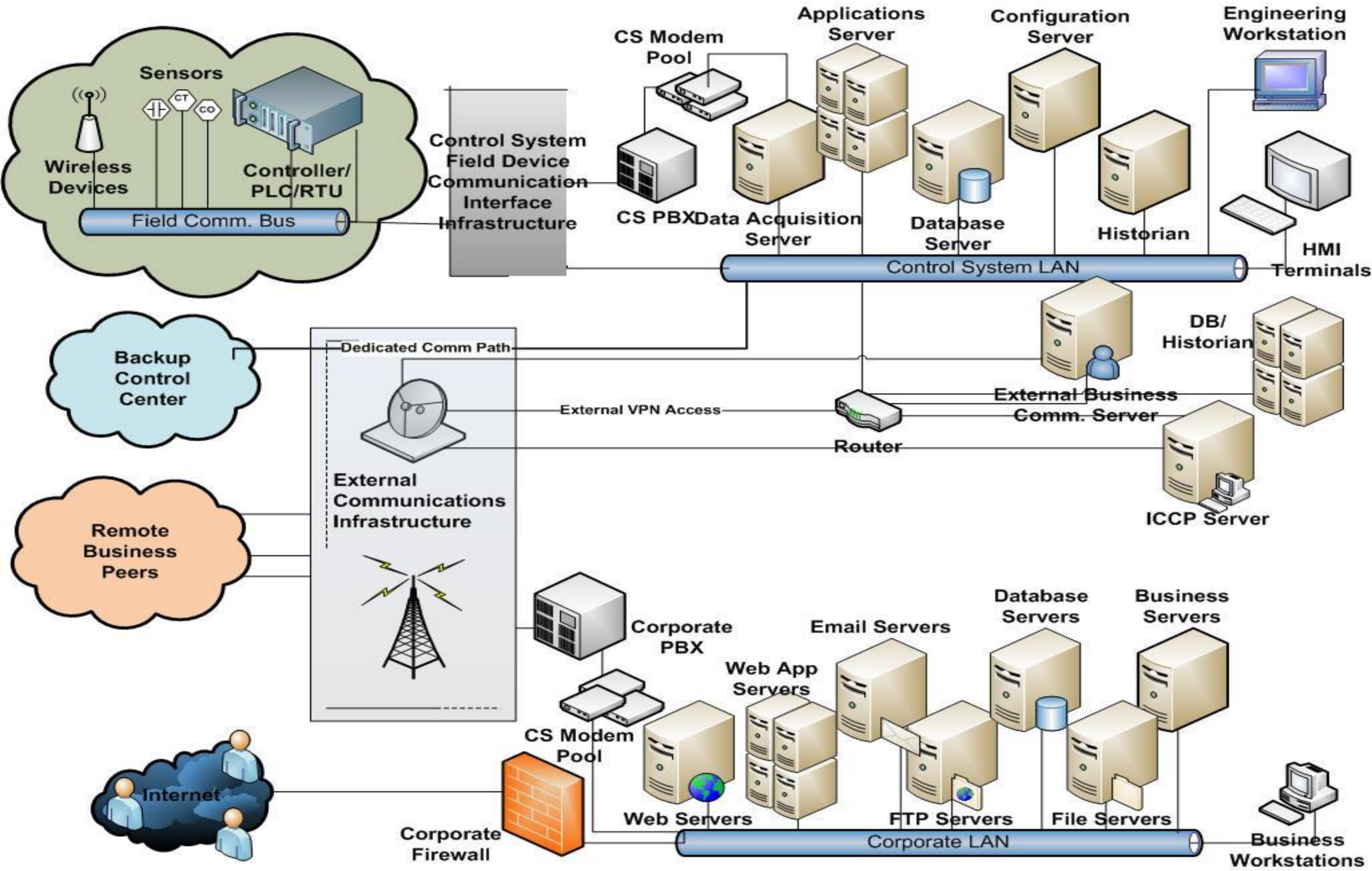
- **Industrial Control System (ICS):** The encompassing term for several types of control systems, including **Supervisory Control and Data Acquisition (SCADA).**

- **HMI:** Human Machine Interface
- **MTU:** Master Terminal Unit
- **PLC:** Programmable Logic Controller
- **RTU:** Remote Terminal Unit



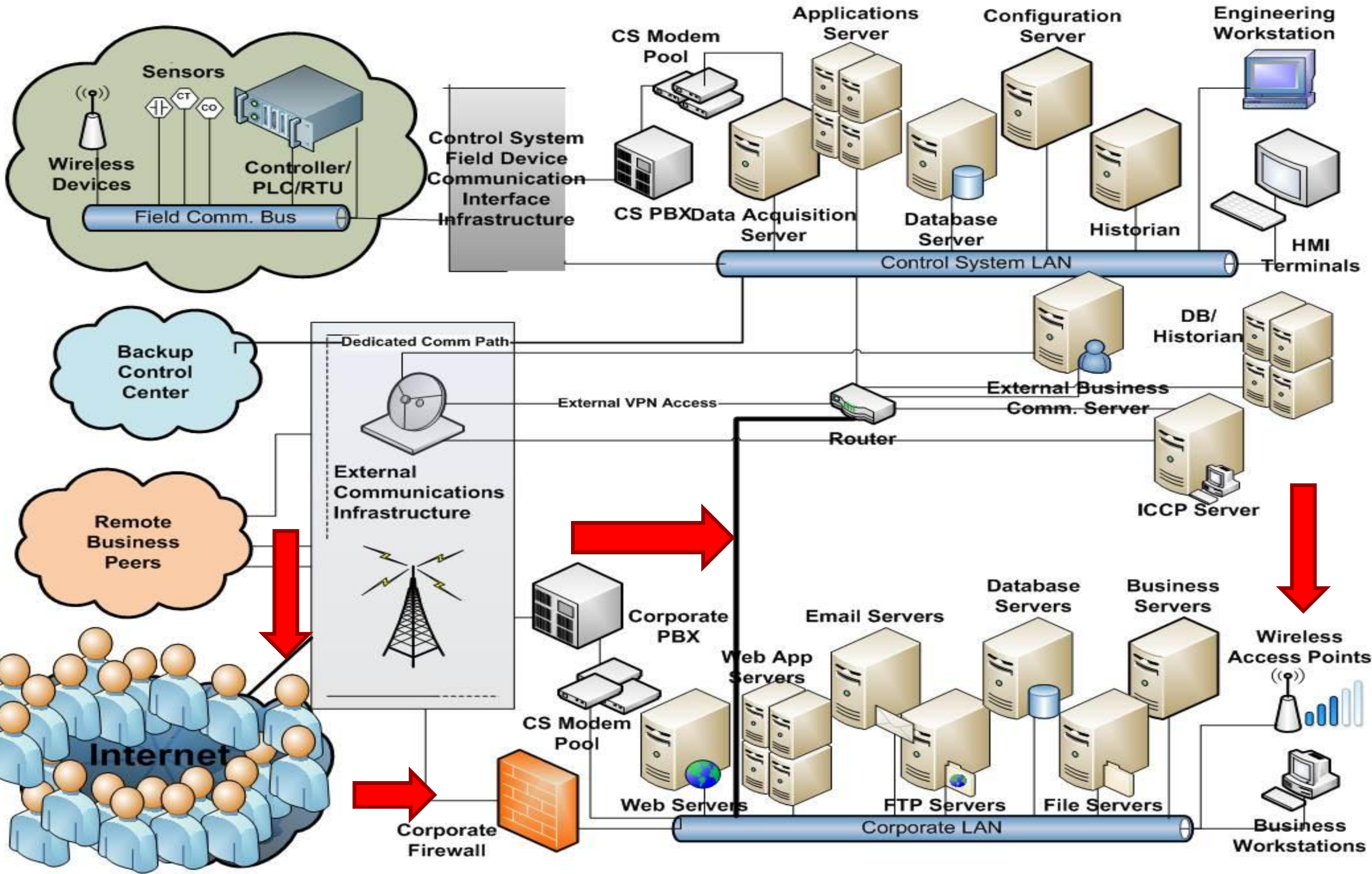
SCADA THEN

Security through obscurity and isolation



SCADA NOW

No longer isolated or obscure



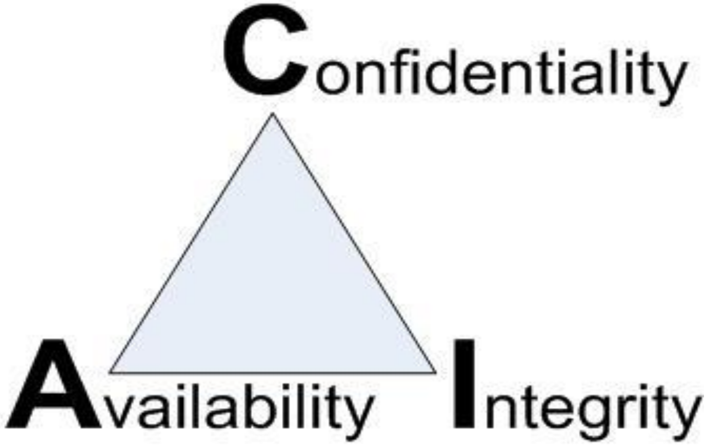
TOP 10 CONTROL SYSTEMS VULNERABILITIES (NERC 2007)

1. Inadequate policies, procedures and culture governing control system security.
2. Inadequately designed control systems networks lack defense-in-depth.
3. Remote access without appropriate access control.
4. System administration mechanisms and software not adequately scrutinized or maintained.
5. Use of inadequately secured wireless communication for control.
6. Use of non-dedicated communication channels for command and control, or use of control system bandwidth for non-command and control purposes.
7. Insufficient use of tools to detect and report on anomalous or suspicious activity.
8. Unauthorized or inappropriate applications or devices on control systems networks.
9. Control Systems command-and-control data not authenticated.
10. Inadequately managed, designed or implemented critical support infrastructure.

1. INADEQUATE POLICIES, PROCEDURES AND CULTURE GOVERNING CONTROL SYSTEM SECURITY

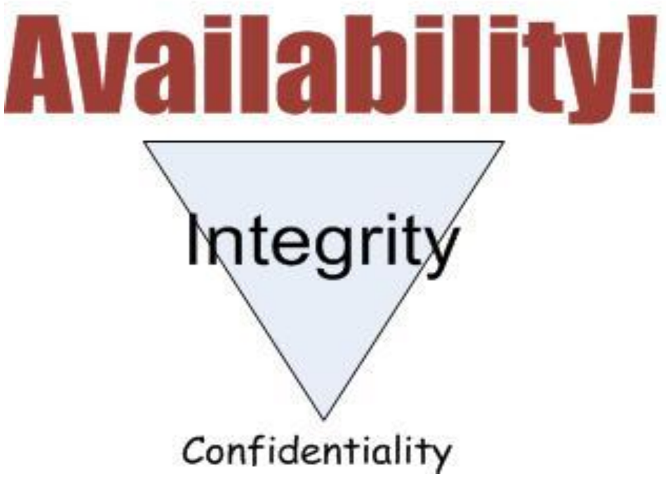
– Traditional IT: CIA Triad

- Equal in importance



– SCADA: Availability

- Integrity = afterthought
- Confidentiality = ?



2. INADEQUATELY DESIGNED CONTROL SYSTEMS NETWORKS LACK DEFENSE-IN-DEPTH.

- Davis-Besse Nuclear Power Plant, 2003. SQL Slammer Worm *disables Safety Parameter Display Systems.*
- Plant firewall blocks Slammer, *contractor network* did not.
- Contractor T1 line *bypasses firewall* to corporate LAN (Windows-based).
- Slammer jumps from corporate to control system LAN.
- Safety Parameter Display System (SPDS), and Plant Processing Computer (PPC) crash, *more than 5 hours to get back online.*

* *Plant was inactive at the time, and both systems had analog backups that were unaffected.*

3. REMOTE ACCESS WITHOUT APPROPRIATE ACCESS CONTROL

- Huntington Beach, CA, 2008. IT consultant *disables pipeline leak-detection for multiple oil platforms* off the coast of California.
- Consultant, not hired permanently by Oil & Gas company, had created *multiple user accounts*.
- For almost two months the consultant used ‘programs, codes and commands’ to impair the company’s systems.
- The systems allowed *remote operation of the platform from corporate* offices.
- The consultant did *most of the damage from his home*, through the corporate connection.

4. SYSTEM ADMIN MECHANISMS AND SOFTWARE NOT ADEQUATELY SCRUTINIZED OR MAINTAINED

COM/DCOM

Configuring DCOM on Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1

Introduction

Microsoft Windows XP Service Pack 2 (SP2) and Windows Server 2003 Service Pack 1 (SP1) include many changes that enhance security. Although these changes resolve problems that were present in earlier versions of Windows, they also prevent SAS DCOM servers from functioning. To enable SAS DCOM functionality, ***you must disable the additional security that is provided by these service packs*****.**

Because enabling DCOM exposes security vulnerabilities that were corrected with Windows XP SP2 and Windows Server 2003 SP1, we recommend that you consider changing your SAS configuration to use IOM Bridge servers instead of DCOM.

If you continue to use DCOM, you will need to perform the following steps:

Disable the Windows Firewall

Configure DCOM Settings on the Server Machine

Configure DCOM Settings on Each Client Machine

5. USE OF INADEQUATELY SECURED WIRELESS COMMUNICATION FOR CONTROL

- Queensland, Australia, 2000. *250 million tons of sewage* leaked into waterway.
- Dispute with contractor after helping to install waste management system.
- Denied employment with the Waste Management Agency.
- Undetected over a *2 month period*, attacker drives around changing valve settings, making at least *46 attempts*.
- Commands were issued to *radio-controlled* sewage equipment.

6. USE OF CONTROL SYSTEM BANDWIDTH FOR NON-COMMAND AND CONTROL PURPOSES

- **Harrisburg, PA, 2006**. *Hackers turn Water Treatment Plant into Spam-Bot.*
- Employee laptop infected with malware via the internet, which then propagates to SCADA system.
- *Control system used to send spam e-mail, host pirated software*.

- **Shelby City, OH, 2009**. Wastewater Treatment Plant employee *indicted, charged with hacking*, for computer misuse.
- Misuse includes: browsing adult websites, soliciting dominatrix, and *uploading nude photos* of himself.

7. INSUFFICIENT USE OF TOOLS TO DETECT AND REPORT ON ANOMALOUS OR SUSPICIOUS ACTIVITY

SAINT®

eEye Digital Security®

Active Tools!

Nessus

metasploit

NMAP.ORG

8. UNAUTHORIZED OR INAPPROPRIATE APPLICATIONS OR DEVICES ON CONTROL SYSTEMS NETWORKS

- Iran, Summer 2009, *Classified electronics data* on US president's helicopter (MarineOne) discovered on public file share.
- Accidentally leaked from contractor computer *via file-sharing network.*
- Iranian computer contained *other sensitive/classified US military documents.*
- Authorities notified in early 2008. *More than a year later data still available* on public peer-to-peer (P2P) networks.

9. CONTROL SYSTEMS COMMAND & CONTROL DATA NOT AUTHENTICATED

- **MODBUS**
  - *Force Listen Only*, Read Device Id, Restart Communication
- **DNP3**:
  - Disable Unsolicited Responses, *Restart from Unauthorized Client*
- **ICCP**:
  - Unauthorized Association Request, *Unauthorized Write Request*
- **CitectSCADA – used by thousands of utilities and plants**
  - ODBC Service Buffer Overflow, allows arbitrary code execution
  - *No authentication required, public exploit available*
- **DATAC RealWin FlexView HMI**
  - Server running on Windows 2000 or XP, *used in over 40 countries*
  - *No authentication required* for arbitrary code execution

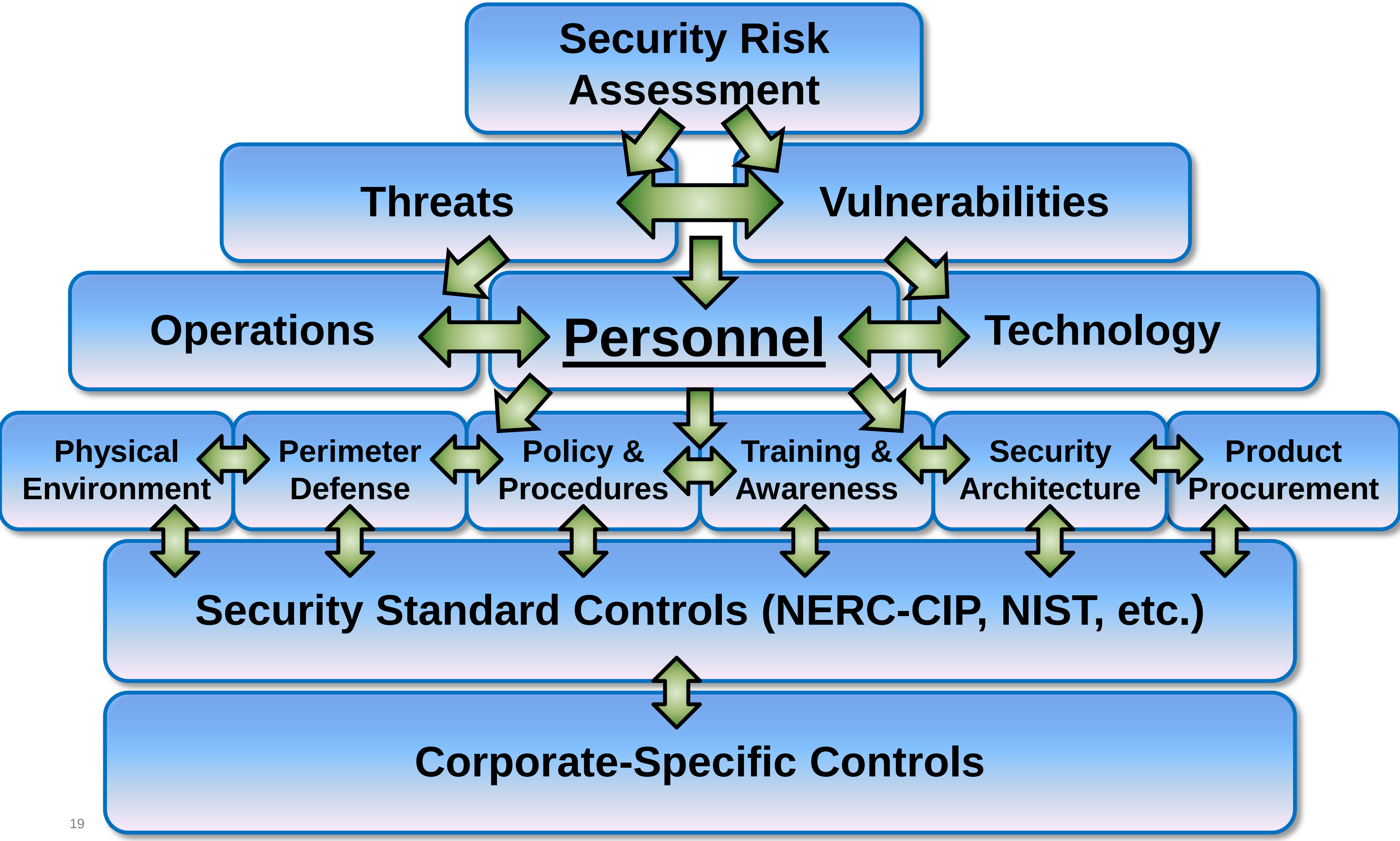
***** ***<u>As of May 2010</u>***

- ***US-CERT/ICS-CERT: 28 SCADA vulnerabilities listed.***
- ***TippingPoint IPS: 60+ filters for SCADA vulnerabilities.***

10. INADEQUATELY MANAGED, DESIGNED OR IMPLEMENTED CRITICAL SUPPORT INFRASTRUCTURE

- Texas City, TX, 2005. BP Oil Refinery, explosion *kills 15, injures 170.*
- Numerous safety recommendations unheeded or ignored by management.
- False instrument readings, ineffective communications, and failed alarms and gauges cause overfilling of fuel tower.
- BP spends *$1 Billion* to upgrade and improve safety.
- 2009, BP fined *$87 million* for failure to comply with 2005 settlement.

SO WHAT CAN BE DONE?



Security Risk Assessment

Threats

Vulnerabilities

Operations

Personnel

Technology

Physical Environment

Perimeter Defense

Policy & Procedures

Training & Awareness

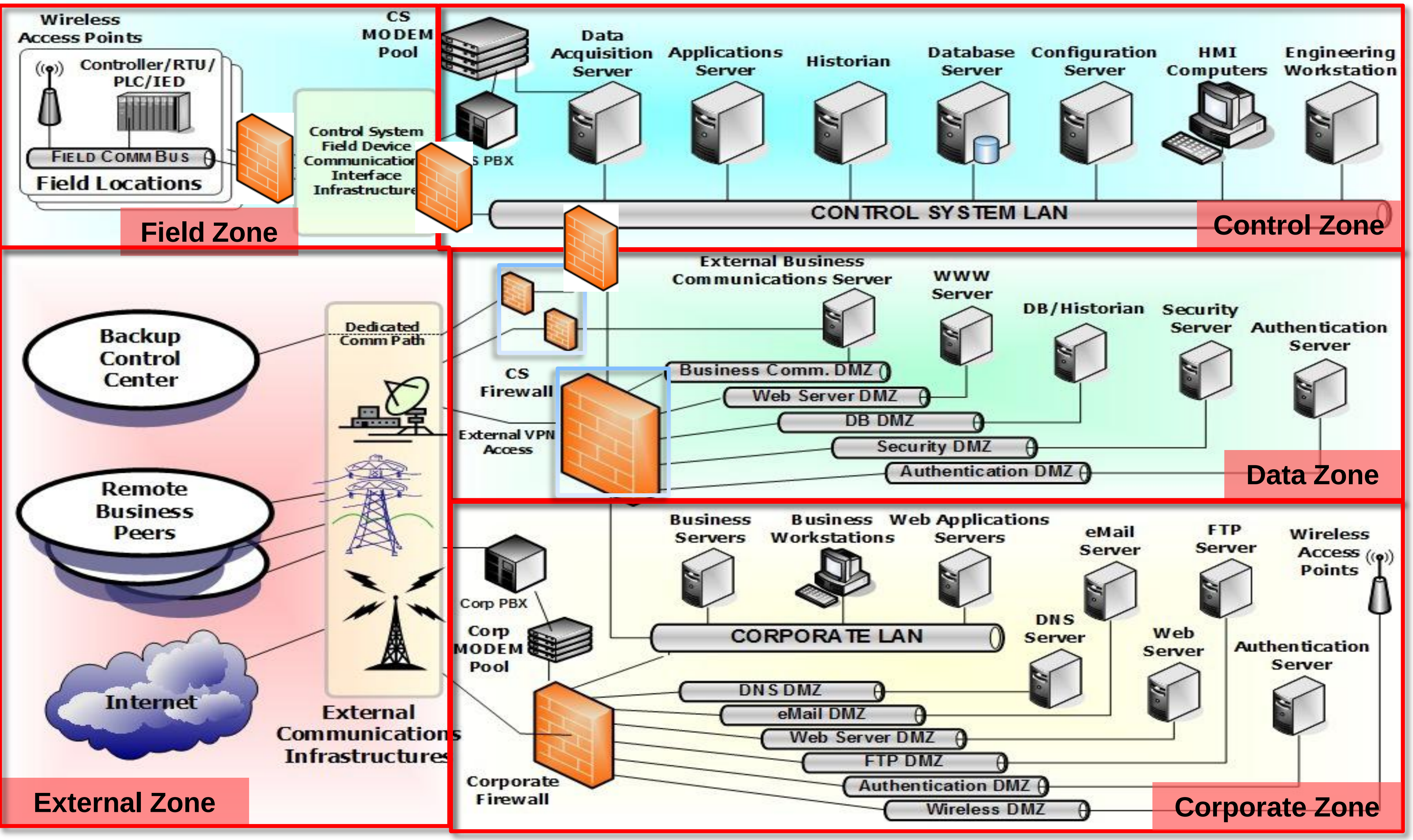
Security Architecture

Product Procurement

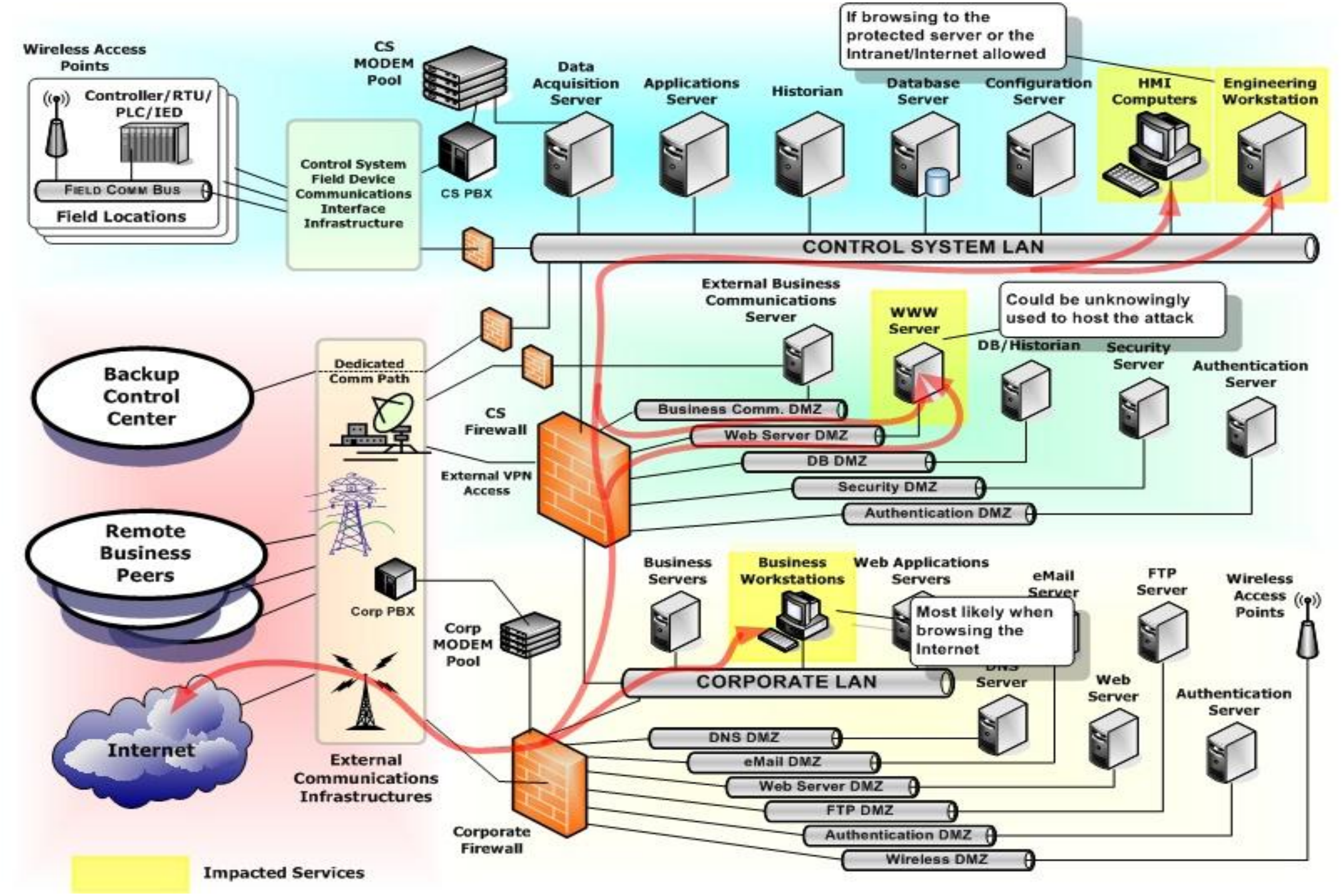
Security Standard Controls (NERC-CIP, NIST, etc.)

Corporate-Specific Controls

ARCHITECT FOR SECURITY



ANATOMY OF AN ATTACK

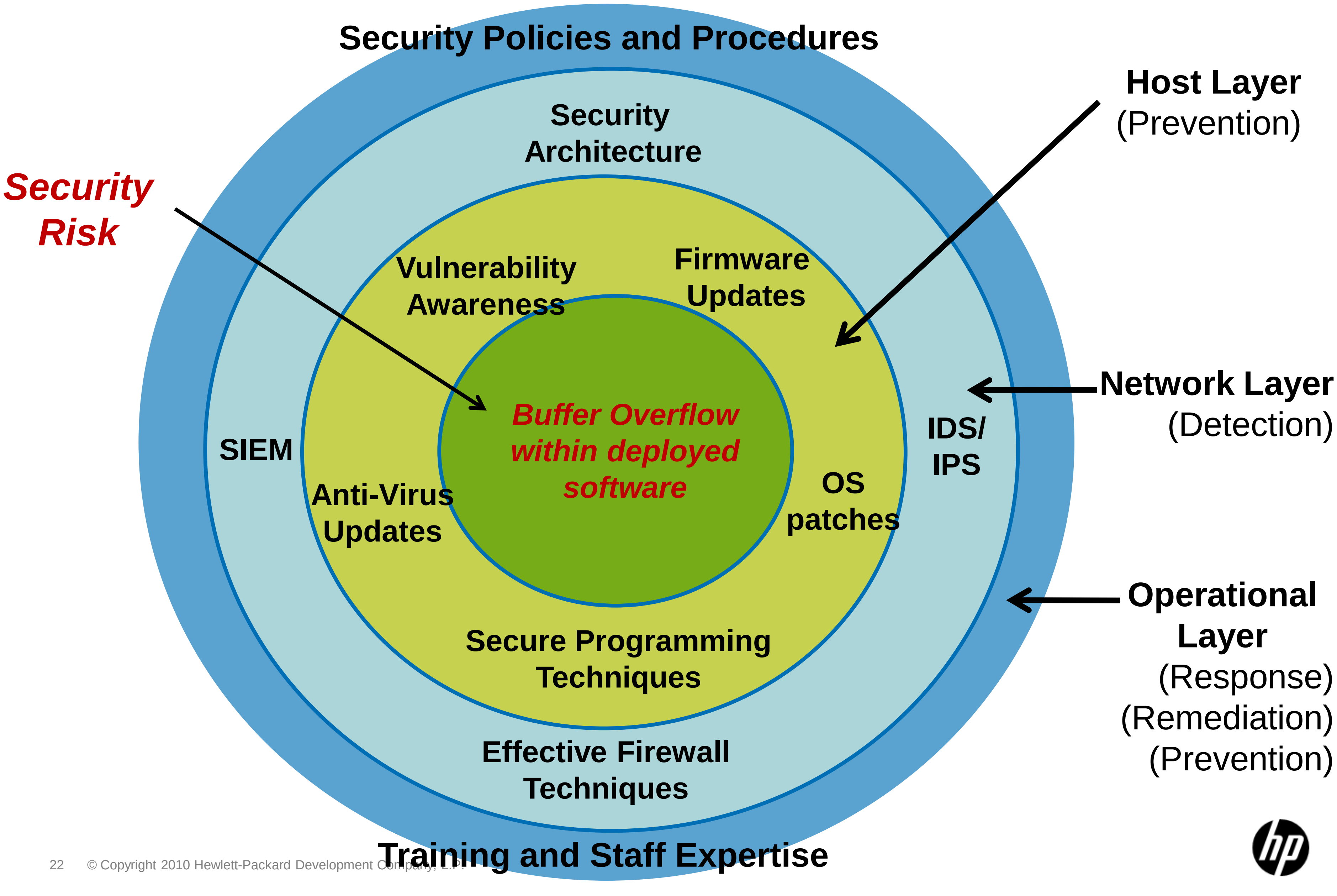


If browsing to the protected server or the Intranet/Internet allowed

Could be unknowingly used to host the attack

Most likely when browsing the Internet

DEFENSE-IN-DEPTH



Security Policies and Procedures

Security Architecture

Security Risk

Vulnerability Awareness

Firmware Updates

Host Layer (Prevention)

Buffer Overflow within deployed software

SIEM

Anti-Virus Updates

OS patches

IDS/ IPS

Network Layer (Detection)

Operational Layer (Response) (Remediation) (Prevention)

Secure Programming Techniques

Effective Firewall Techniques

Training and Staff Expertise

ADDITIONAL RESOURCES

- US-CERT/Control Systems Security Program (CSSP)
  - http://www.us-cert.gov/control_systems/
- NERC Critical Infrastructure Protection (CIP:002 – CIP:009)
  - http://www.nerc.com/page.php?cid=2|20
- NIST 800-53, Rev. 3. August 2009
  - http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf
- SCADApedia (Digital Bond)
  - http://www.digitalbond.com/wiki/index.php/Main_Page
- Repository of Industrial Security Incidents (RISI)
  - http://www.securityincidents.org/
- Center for SCADA Security (Sandia National Labs)
  - http://www.sandia.gov/scada/
- DHS Aurora Attack Demonstration Video
  - http://www.cnn.com/2007/US/09/26/power.at.risk.index.html

Q&A

CONTACT INFORMATION

- Garett Montgomery
- Security Researcher, DVLabs, TippingPoint
- gmontgomery@tippingpoint.com
- garett.m.montgomery@hp.com

- TippingPoint IPS: www.tippingpoint.com
- DVLabs: dvlabs.tippingpoint.com

CONTACT INFORMATION

– Garett Montgomery

– Security Researcher, DVLabs, TippingPoint

– gmontgomery@tippingpoint.com

– garett.m.montgomery@hp.com

– TippingPoint IPS: www.tippingpoint.com

– DVLabs: dvlabs.tippingpoint.com